NASA Policy Directive

NPD 1660.1A
Effective Date: February 27, 2002
Expiration Date: February 27, 2012

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Counterintelligence (CI) Policy (Revalidated 12/19/2006)

Responsible Office:

1. Policy

a. It is NASA policy to establish and maintain a CI program. This program shall be conducted pursuant to the National Aeronautics and Space Act of 1958, as amended, and in conformance with other applicable laws, Executive Orders, Presidential Decision Directives, Federal Regulations, and NASA directives.

b. The Office of Security Management and Safeguards (OSMS) shall manage the NASA CI program. The CI objective is to detect, deter, and neutralize the potential threat posed by Foreign Intelligence Services (FIS), other foreign entities, and acts of terrorism. The OSMS will utilize information and undertake approved safeguard measures to protect the Agency against espionage, other intelligence activities, sabotage, foreign or domestic terrorism, or threats conducted for or on behalf of foreign powers, organizations, or persons, and directed toward personnel, facilities, operations, or administratively controlled, export controlled, national security classified or proprietary information.

c. All CI activities shall be conducted fairly, objectively and with full regard for applicable laws and policies.

2. Applicability

a. This NPD is applicable to all NASA programs, projects, operations, personnel, and other activities conducted by or for NASA at NASA Headquarters and NASA Centers, including Component Facilities, and to any contractor personnel or other person or entity to the extent provided in the contract or other governing instrument.

b. Nothing in this directive shall be construed as limiting the authorities of the Inspector General under the Inspector General Act of 1978, as amended.

c. For purposes of this directive "counterintelligence" means, but is not limited to, information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, and international or domestic terrorist activities.

3. Authority

a. 42 U.S.C. 2473 (c), Section 203 (c) of the National Aeronautics and Space Act of 1958, as amended.

b. 42 U.S.C. 2455, Section 304 of the National Aeronautics and Space Act of 1958, as amended.

c. NPR 1000.3, the NASA Organization.

4. Reference

a. 5 U.S.C. Section 552a, The Privacy Act of 1974 (PublicLaw 93-579), as amended.

b. 5 U.S.C. App., Inspector General Act of 1978, as amended.

c. 18 U.S.C. Sections 1831 - 1839, Title I of the Economic Espionage Act of 1996 (Public Law 104-294, October 11, 1996), as amended (as related to CI and Counterterrorism (CT)).

d. 50 U.S.C. 401a, Section 3 of the National Security Act of 1947, as amended.

e. 50 U.S.C. 402a, Section 811 of the Intelligence Authorization Act for Fiscal Year 1995 (Public Law 103-359, October 14, 1994), as amended.

f. Executive Order 10450, Security Requirements for Government Employees, April 27, 1953 (3 CFR 1949 - 1953 Compilation), as amended.

g. Executive Order 12333, United States Intelligence Activities, December 4, 1981 (3 CFR 1981 Compilation), as amended.

h. Executive Order 12958, Classified National Security Information, April 17, 1995 (3 CFR 1995 Compilation), as amended.

i. Executive Order 12968, Access to Classified Information, August 2, 1995 (3 CFR 1995 Compilation), as amended.

j. Presidential Decision Directive 39, Counterterrorism Policy, June 21, 1995, as amended.

k. Presidential Decision Directive 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998, as amended.

l. Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998, as amended.

m. NPR 1620.1, Security Procedures and Guidelines

n. NPR 1660.x, Counterintelligence Procedures and Guidelines.

o. NPR 2810.1, Security of Information Technology

5. Responsibility

a. The Assistant Administrator (AA) for Security Management and Safeguards has the responsibility for the overall policy, direction, and oversight for the NASA CI program. This responsibility includes the following:

(1) CI LIAISON --
The AA or designee(s) will serve as the liaison with the U.S. Intelligence Community on matters concerning terrorism and foreign intelligence relating to CI and CT activities. This responsibility focuses on the utilization and dissemination of CI & CT threat information affecting NASA's personnel, technology, programs/projects, operations and facilities. Center CI offices will receive information from OSMS and will maintain local liaison with appropriate Federal and State agencies, contractors and Center personnel.

(2) CI INVESTIGATIONS -- (Administrative Inquiries, Preliminary Inquiries and Joint Investigations)
The AA or designee(s) will maintain and centrally control the NASA CI investigative management system. The purpose of CI investigations is to determine the facts, using the least intrusive investigative means, concerning incidents or allegations of the compromise or suspected compromise of administratively controlled, export controlled, classified or proprietary information; and the protection of personnel, facilities, and operations from the threats posed by espionage and acts of terrorism conducted for or on behalf of foreign or domestic powers or organizations, persons, and domestic or international terrorist activities.

(a) Administrative inquiries will be conducted concerning misconduct or incidents that impact the proper protection of personnel, facilities, operations, administratively controlled, export controlled and proprietary information in a CI or counterterrorism context. Administrative inquiries may be initiated at the request of the Federal Bureau of Investigation (FBI), upon direction from appropriate Center Management, or when deemed prudent by the Center CI Agent. As appropriate, these inquiries will be coordinated with the offices referenced in paragraph 5.b. below.

(b) Preliminary inquiries will be conducted based upon indicators of foreign intelligence methodology or indications of espionage or terrorism directed at personnel, facilities, operations, administratively controlled, export controlled, classified, or proprietary information. Preliminary inquiries will usually be coordinated with the FBI prior to the mandatory reporting requirements specified in Section 811 of the Intelligence Authorization Act for Fiscal Year 1995.

(c) Joint investigations will be conducted with other Federal agencies as appropriate.

(3) CI EDUCATION AND AWARENESS TRAINING --
OSMS will develop and conduct informative briefings for selected NASA audiences/activities (including programs/projects/operations) concerning current threats posed by terrorism, FIS, and others who attempt to obtain unauthorized NASA administratively controlled, export controlled, proprietary, or classified information/technology. OSMS will identify and establish the curriculum and training standards for NASA CI personnel.

(4) CI ANALYSIS AND COUNTERTERRORISM --
OSMS will conduct an analysis program using acquired FIS and terrorism threat information for specific threat briefings to targeted NASA personnel or activities (including programs/projects/operations). The results of these analyses will also be used to create, change, or enhance physical and/or personnel security countermeasures

designed to minimize vulnerabilities and confront any threats. Center CI offices will receive analysis from OSMS and will also undertake appropriate steps to address and analyze local CI threats.

b. Under the applicable authorities, the AA or designee(s) will be the focal point for making "Section 811" referrals to the FBI. The AA or designee also serves as the Executive Secretary of the NASA Security Council. The AA will coordinate CI issues, as appropriate, with the NASA Inspector General, the NASA Chief Information Officer, the Associate Administrator for External Relations, the NASA General Counsel, and other NASA officials as necessary to carry out the CI mission.

c. ACCESS TO RECORDS, DOCUMENTS, PERSONNEL, AND PREMISES IN SUPPORT OF CI ACTIVITIES
All NASA personnel and organizations, other Federal personnel or military detailees, and any contractor or grantee or other entity as provided in the governing agreement or instrument and who are located at any NASA installation, shall cooperate fully with the OSMS and its representatives, to the extent permitted by law. During the conduct of administrative inquiries, preliminary inquiries, joint investigations, or other CI activities, such cooperation will include the following, to the extent permitted by law:

(1) Complete and free access to NASA premises, employees, files and documents, but not including the Office of the Inspector General (OIG).

(2) Access to records, premises, and employees pursuant to access provisions governing NASA's arrangements with offsite entities.

(3) Statements, both oral and written, including statements under oath or affirmation, with due regard to Privacy Act considerations.

(4) Technical consultation, examination, and assistance regarding information or evidence being developed.

(5) Such other assistance as may be required in order to complete the inquiry or investigation.

d. The OSMS CI Program Manager (CIPM) has overall responsibility for CI operations, investigations, and the coordination and oversight of CI training at each NASA Center. The CIPM will perform all appropriate investigative functions under the policy, guidance, direction and supervision of the AA, and maintain (except for OIG) records on all CI allegations, investigations, incidents, and their resolution.

e. The CI offices at each NASA Center will conduct CI liaison; CI investigations; CI education and awareness training; CI analysis and CT analysis and prevention for NASA personnel, onsite contractors and visitors, programs/projects, operations and facilities.

f. NASA Center Directors (CD). NASA CD's are responsible for the following:

(1) Creating and maintaining a dedicated CI office responsible for administering the NASA CI Program at the Center level.

(2) Assuring that all allegations of espionage, terrorism threats, or incidents providing counterintelligence indicators of the loss or potential loss of administratively controlled, export controlled, proprietary, or classified national security information are reported expeditiously to the OSMS, and that NASA Centers and Component Facilities fully cooperate in the conduct of inquiries, investigations, and other NASA CI activities, to the extent permitted by law.

(3) Assuring that Center and Component Facility personnel attend mandatory CI awareness and threat briefings.

g. NASA Employees. Any NASA employee, who observes or becomes aware of the deliberate or suspected compromise of classified national security information will promptly report such information personally to their Center CI Office. If unclassified but sensitive information appears compromised by or on behalf of foreign or domestic powers, organizations or persons, employees shall report such information to their Center CI Office. If an employee becomes aware of information pertaining to international or domestic terrorist activities, employees shall also report to the Center CI Office. If the information indicates a computer compromise or other cyber intrusion, the OIG will be promptly notified. In order to ensure free and unimpeded access to the CI personnel, an employee may ask for confidentiality.

6. Delegation of Authority

None.

7. Measurements

The AA will provide an annual report providing metrics and other information concerning the results of CI investigations, terrorism analysis threats, liaison contacts, "Section 811" referrals, and foreign traveler debriefs to the NASA Administrator.

8. Cancellation

NPD 1660.1, NASA Counterintelligence (CI) Policy, February 27, 2002.

REVALIDATED 12/19/2006, ORIGINAL SIGNED BY:

/s/ Sean O'Keefe
Administrator

Attachment A: (Text)

None.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov